Operational Instruction

Operational Instruction: OI 2019
Area: Information Technology
Effective Date: 04/02/2003
Approved: _____
David Stevenson, Associate Director,
Office of Information Technology
Chief Technology Officer (Acting)

INTERNAL ACCOUNT MANAGEMENT PROCEDURE

I. COVERAGE

This policy covers all permanent, temporary, and part-time Court Services and Offender Supervision Agency (CSOSA), Office of Information Technology Services employees, as well as interns, and contractors. The term "employee" as used in this policy covers all of these categories.

II. BACKGROUND

The Office of Information Technology (OIT) is responsible for creating, managing and distributing automated data processing accounts.

III. POLICY

The Office of Information Technology will use the steps in this procedure to create automated data processing accounts. This document is supporting documentation for the Agency Account Management Policy (PS 2003).

IV. AUTHORITIES, SUPERCEDURES, REFERENCES, AND ATTACHMENTS

A. Authorities:

- Court Services & Offender Supervision Agency Account Management Policy

B. Supercedures:

None.

C. Procedural References:

None.

D. Attachments:

Appendix A. General Procedures

Appendix A

I. LAN/E-Mail Accounts

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

Community Supervision Services (CSS)	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Intern for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Intern for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The New Employee letter, sent via e-mail from Office of Human Resources (OHR), will be sent to the appropriate supervisor/manager of CSS/Office of the Director and IT Security with a copy to IT Help Desk indicating the start date of the new employee.
- ✓ The letter will direct the supervisor/manager to the website with a link to the Computer Access and New Employee Setup forms. They will be informed to complete the appropriate form(s) and forward to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Help Desk Staff will generate a ticket based upon the information received from OHR. The ticket will be assigned to the Access Control Group.
- ✓ The automatic e-mail notification will indicate that this is a request for a new employee account and will be sent to both the IT Help Desk and IT Security staff.
- ✓ The Help Desk staff will create the accounts but disable them until approval is received from IT Security.
- ✓ IT Security will send an email to the IT Help Desk notifying them when approval has been granted. IT Security will also contact the employee's supervisor notifying them that access has been granted and ask him/her to have their new person contact the Help Desk for account activation.
- ✓ After the account has been activated the Help Desk staff will then close the ticket.

Appendix A

Sample Letter from OHR announcing new employee

WELCOME THE FOLLOWING NEW EMPLOYEES
[CSS/Department]
NAME: ***Employee Name***
TITLE: ***Employee Title***
STAFF: ***Department***
STARTS: ***Staring Date***
MANAGER: ***Manager's Name***

Please make the necessary arrangements to plan for their arrival on the dates noted above. All administrative/worksite arrangements are to be coordinated with the hiring staff prior to the employee's first day of employment. Any Human Resources issues should be forwarded to OHR. The timekeeper will be notified under a separate notice due to privacy act information.

In addition, the hiring office must complete the computer access form and forward directly to the IT Security Officer at 633 Indiana Ave., Room 734 within AT LEAST 7 calendar days before the employee is to report for duty. The form must include the office, room number and telephone number that will be assigned to the new employee and signed by the appropriate manager. If the form is not submitted by the required time the IT Staff cannot guarantee that a computer and telephone will be available on the employee's first day. Any specific questions concerning the form should be directed to the IT Staff.

OHR Servicing Specialist: Sherry Harrison, Human Resources Specialist 220-5605
Donna Sharp, Human Resources Assistant 220-5617
808 17th St., NW, Suite 820
Washington, DC 20006
202-220-5601 (main #)
202- 220-5615 (fax#)

****URL for Computer Access form and New Employee Setup form*****

Appendix A

II. Remote Access (Virtual Private Network (VPN) or Web-Based)

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket and assign the ticket to the Access Control Group.
- ✓ If the request is approved, IT Security will assign the ticket to the Account Management Group.
- ✓ An automatic e-mail notification will indicate that this is a request for remote access VPN or Web-based access and will be sent to the IT Help Desk and IT Security staff. (**Note: VPN is for OIT Staff, External users and Pre-trial Services Agency (PSA) only. Web-based access is for CSOSA users only)**
- ✓ **For web-based accounts**, IT Help Desk will activate the account.
  - ✓ The IT Help Desk Staff will send an e-mail to the requestor, notifying them of the installation process. VPN account holders will be sent the VPN installation documentation. Web-based account holders will be notified to attend Telecommuting Training in the CSOSA Training Center and sent the documentation for Web-based account holders. The notification to the Web-based account holders will read as follows:

    Your remote computer access has been approved. The installation documentation for this access is attached to this e-mail. Please attend the Telecommuting Training in the CSOSA Training Center prior to using this access. You must attend training prior to receiving assistance for installing or using this service from the IT Help Desk.

    Thanks

  - ✓ IT Help Desk will activate the web-based account.

Appendix A

- ✓ **For VPN accounts**, IT Security will activate the account after the customer has set up VPN and informed them that the account has been registered.
- ✓ The ticket will then be closed by IT Security.

Appendix A

III. SMART (Supervision and Management Automated Tracking System)

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox.
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control group.
- ✓ The Notification message will indicate that this is a request for SMART access.
- ✓ IT Security will assign the ticket to the Account Management group once approval has been granted.
- ✓ An email notification will be sent to the Help Desk Staff when the ticket is reassigned.
- ✓ For New Employees: Once access has been approved, IT Help Desk Staff will create a SMART account based upon the Smart Guidelines and contact the requestor supplying them with the user account and steps on changing their password.
- ✓ For Existing Employees: Once access has been approved, IT Help Desk Staff will create a SMART account based upon the Smart Guidelines and contact the requestor supplying them with the user account and steps on changing their password.
- ✓ The IT Help Desk Staff will close the ticket when completed.

Appendix A

IV. Justice Information System (JUSTIS)

JUSTIS is located under the CSOSA applications via the intranet.

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for JUSTIS access.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the requestor supplying them with the additional information needed to access the program (JUSTIS Application form).
- ✓ Once the JUSTIS application has been completed, IT Security will send the form to the JUSTIS help Desk for processing.
- ✓ IT Security will update the help Desk ticket, with the date and time the information was sent to the JUSTIS help Desk.
- ✓ Once the appropriate account has been secured, IT Security will contact the requestor supplying them with the user account information.

Appendix A

- ✓ The ticket will then be closed by IT Security.

Procedures for password resets:

- ✓ The Help Desk will generate a ticket indicating that a password reset is required.
- ✓ The ticket will be assigned to the Access Control group queue.
- ✓ The Notification message will indicate that this is a request for a password reset for JUSTIS.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the appropriate people to have the password reset.
- ✓ IT Security will update the Help Desk ticket, with the date and time the request was sent to the JUSTIS Help Desk.
- ✓ Once the password has been reset, IT Security will notify the requestor and close the ticket.
- ✓ The ticket will then be closed by IT Security.

Appendix A

V. Washington Area Law Enforcement System (Wales)/ National Crime Information Center (NCIC)

Wales/NCIC is located under the CSOSA applications via the intranet.

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for Wales/NCIC access.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the CSOSA Office of Security to receive clearance information on the requestor.
- ✓ IT Security will contact the requestor and supply dates for training.
- ✓ The account requestor will fill out the Wales/NCIC application during the training class.
- ✓ Once the Wales/NCIC application has been completed, IT Security will send the form to the Metropolitan Police Department (MPD) for processing.

Appendix A

- ✓ IT Security will update the Help Desk ticket, with the date and time the information was sent to MPD.
- ✓ Once the appropriate account has been secured, IT Security will contact the requestor supplying them with the user account information.
- ✓ The ticket will then be closed by IT Security.

Procedures for password resets:

- ✓ The Help Desk will generate a ticket indicating that a password reset is required.
- ✓ The ticket will be assigned to the Access Control group queue.
- ✓ The Notification message will indicate that this is a request for a password reset for WALES/NCIC.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the appropriate people to have the password reset.
- ✓ Once the password has been reset, IT Security will notify the requestor.
- ✓ The ticket will then be closed by IT Security.

Appendix A

VI. Courts Information Systems (CIS)

Access will be granted via the JUSTIS application only. JUSTIS is located under the CSOSA applications via the intranet.

Computer Access form (CSOSA/IT-0001) should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for CIS access.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the requestor supplying them with the additional information needed to access the program (JUSTIS Application form).
- ✓ Once the JUSTIS application has been completed, IT Security will send the form to the JUSTIS Help Desk for processing.
- ✓ IT Security will update the Help Desk ticket, with the date and time the information was sent to the JUSTIS Help Desk.

Appendix A

- ✓ Once the appropriate account has been secured, IT Security will contact the requestor supplying them with the user account information.
- ✓ The ticket will then be closed by IT Security.

Procedures for password resets:

- ✓ The Help Desk will generate a ticket indicating that a password reset is required.
- ✓ The ticket will be assigned to the Access Control group queue.
- ✓ The Notification message will indicate that this is a request for a password reset for JUSTIS.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the appropriate people to have the password reset.
- ✓ IT Security will update the Help Desk ticket, with the date and time the request was sent to the JUSTIS Help Desk.
- ✓ Once the password has been reset, IT Security will notify the requestor and close the ticket.

The ticket will then be closed by IT Security.

Appendix A

VII. Sentry

Sentry is located under the CSOSA applications via the intranet.

Computer Access form should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for SENTRY access.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will forward the Rules of Behavior form to the requestor and gather necessary background investigation data from CSOSA Security Department which is required by the Bureau of Prisons (BOP).
- ✓ Once the appropriate account has been secured, IT Security will contact the requestor supplying them with the user account and any additional information needed to access the program.
- ✓ The ticket will then be closed by IT Security.

Procedures for password resets:

Appendix A

- ✓ The Help Desk will generate a ticket indicating that a password reset is required.
- ✓ The ticket will be assigned to the Access Control group queue.
- ✓ The Notification message will indicate that this is a request for a password reset for SENTRY.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the appropriate people to have the password reset.
- ✓ Once the password has been reset, IT Security will notify the requestor.
- ✓ The ticket will then be closed by IT Security.

Appendix A

VIII. Jail and Community Corrections System (JACCS)

JACCS is located under the CSOSA applications via the intranet.

JACCS is a replacement to the DC Dept. of Corrections inmates tracking system known as CRYSIS. This system was accessible through WALES utilizing transaction Ids (DMAA) to find parolee/inmate location, Full Term Date, etc. To find a split-sentence or revoked or warrant-executed client's whereabouts use JACCS. CRYSIS functionality will continue to be delivered thru JACCS.

Computer Access form should be signed by the appropriate person as listed below:

CSS FTE's	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Office of the Director FTE's	Department Manager
All Contractors	Director of Procurement or Contractor Representative
Interns for CSS	Supervisory Community Supervision Officer (SCSO) or Branch Manager
Interns for Office of the Director	Department Manager

Procedures for new accounts:

- ✓ The Computer Access form http://csosaweb will be filled out and signed by the appropriate person(s) and forwarded to IT Security at 633 Indiana Avenue, Room 734.
- ✓ The OIT Administrative Assistant will time and date stamp the form upon receipt and place the form in the IT Security mailbox. (Mail will only be opened when the form is visible. Personal mail will not be opened).
- ✓ IT Security will create a ticket.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for JACCS access.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ Once access has been approved and the appropriate account has been secured, IT Security will contact the requestor supplying them with the user account and any additional information needed to access the program.
- ✓ The ticket will then be closed by IT Security.

Appendix A

Procedures for password resets:

- ✓ The Help Desk will generate a ticket indicating that a password reset is required.
- ✓ The ticket will be assigned to the Access Control Group.
- ✓ The Notification message will indicate that this is a request for a password reset for JACCS.
- ✓ An email notification will be sent to the Help Desk Staff and IT Security when the new ticket is created.
- ✓ IT Security will contact the appropriate people to have the password reset.
- ✓ Once the password has been reset, IT Security will notify the requestor.
- ✓ The ticket will then be closed by IT Security.

Appendix A

IX. Drug Test Management System (DTMS) [Prism Drug Reports]

Procedures for new accounts

- ✓ If the request for a new account comes via email, IT Help Desk Staff will generate a ticket and assign it to the PSA Help Desk Group.
- ✓ The email will be forwarded to PSA Help Desk.
- ✓ IT Help Desk Staff will then close the ticket with a note in the closure details that the request was sent to PSA Help Desk.
- ✓ If the request comes via telephone, the IT Help Desk Staff will generate a ticket and assign it to the PSA Help Desk Group.
- ✓ IT Help Desk Staff will send an email to the PSA Help Desk with all of the required information.
- ✓ IT Help Desk Staff will then close the ticket with a note in the closure details that the request was sent to PSA Help Desk.

X. PRISM (Pretrial, Probation and Parole Real-time Information Systems)

Procedures for new accounts

- ✓ If the request for a new account comes via email, IT Help Desk Staff will generate a ticket and assign it to the PSA Help Desk Group.
- ✓ The email will be forwarded to PSA Help Desk.
- ✓ IT Help Desk Staff will then close the ticket with a note in the closure details that the request was sent to PSA Help Desk.
- ✓ If the request comes via telephone, the IT Help Desk Staff will generate a ticket and assign it to the PSA Help Desk Group.
- ✓ IT Help Desk Staff will send an email to the PSA Help Desk with all of the required information.
- ✓ IT Help Desk Staff will then close the ticket with a note in the closure details that the request was sent to PSA Help Desk.

XI. Account Deletion and Deactivation

- ✓ IT Security will create a ticket when they have received information on terminations, resignation or dismissal of an employee (OHR checkout, etc). The ticket must state the

Appendix A

date that the account must be disabled/deleted. When accounts must be disabled/deleted immediately, IT Security will contact the Help Desk via telephone.

- ✓ The ticket for LAN, E-mail and SMART accounts will be assigned to the Account Management Group. The ticket VPN access or other accounts will be assigned to the Access Control Group.
- ✓ The automatic e-mail notification will indicate that this is a request for Account Deletion and will be sent to the IT Help Desk and IT Security staff.
- ✓ IT Security will send an e-mail notification to the administrators of external systems used by the employee (i.e. PSA Help Desk for DTMS and PRISM, JUSTIS, WALES/NCIC, Sentry, CIS, JACCS, etc.)
- ✓ IT Help Desk will disable the LAN, E-mail, and SMART accounts close of business on the date identified by IT Security in the ticket. The ticket will be updated with the time and date the account was disabled and/or deleted. The accounts will be deleted after 5 working days.
- ✓ The IT Help Desk will assign the ticket to the Access Control Group.
- ✓ IT Security will disable the VPN access close of business on the date identified by IT Security in the ticket. The account will be deleted after 5 working days. The ticket will be updated with the time and date the account was disabled and/or deleted.
- ✓ IT Security will verify that all CSOSA accounts have been deleted and close the tickets.